The Use of the Blockchain Protocol by Public Administration as an Accomplishment of Efficiency in the Public Service

Felipe Rangel da Silva

Dept. of Master in Law (Student), Centro Universitário de Maringá UNICESUMAR

Av. Guedner, n. 1610, Maringá, PR, Brazil

Rodrigo Valente Giublin Teixeira

Dept. of Master in Law (Professor), Centro Universitário de Maringá UNICESUMAR

Av. Guedner, n. 1610, Maringá, PR, Brazil

Abstract

Bitcoin emerged as a proposal to revolutionize the current financial system. Due to its reliability, it has become popular and has since caught the attention of governments and world leaders. However, what can cause even more impact, not only in financial matters, is one of its components that gives rigidity and veracity to the information conducted within the application: the protocol blockchain. This mechanism of data storage and processing, compared to an open book, can reinvent the exchange and storage of information on the internet. It is already being used by companies to increase productivity and, mainly, to guarantee security against fraud and external attacks, such as ransomwares. Except for the complexity of technical issues that will not be determined due to the thematic limitation, this study proposes to indicate the use of the protocol blockchain as a possibility of security guarantee of public data also by the public initiative, in order to assure more efficiency of the service provided.

Keywords: Blockchain, public administration, efficiency, internet safety

1. Introduction

The changes announced by the emergence of Bitcoin, a digital currency that exceeds international barriers and brings the world closer, as in a grand finale of globalization, are

numerous. Because of the blockchain, the technology developed that gave the conception of this coin, such changes lead us to characterize them, and undoubtedly, refer to them as a Revolution.

Much has already been written about its development and the possibilities that are open in economic terms for digital coins. Nevertheless, even more relevant is the Blockchain, the system that provides reliability in transactions and, especially, the areas in which this technology can be implemented. May these areas be in the private sector (as it already occurs in the use and popularization of digital currencies), or in the public one, which will be addressed during the present research.

It is worth to mention that the development of digital coins and the protocol of security and veracity of information inherent to these, has been taken into extreme proportions. Authors from various fields, such as economics, sociology and evidently information technology, announce that in a few years, more precisely, no more than two decades, we will talk about the blockchain as we speak of the internet today, with a certain dominion spread among the population; as well as the handling and programming within electronic systems that will make use of such technology, will be widespread and inherent to all users and/or consumers.

As it will be explored - with limited technical clarifications to the basic understanding of the operation of the technology in question, given the approach taken to the legal impact - the blockchain protocol can serve humanity in several functions. For instance, it has the capacity to replace, with much greater efficiency, the electronic information storage systems, which demand a high investment and maintenance cost, especially regarding the energy consumption. Being it is no longer appropriate to be approached, except in the context of digital currencies, it should be taken into consideration the proposal of the hypotheses in which the protocol of storage and information transactions - not necessarily monetary - can be applied to improve the lives of Internet users, that is, in some years of the entire world population, since it is headed towards an almost complete universalization of the Internet's use.

Undoubtedly, the private sector is prevailing when it comes to technological development. Therefore, the blockchain protocol arises to support the solution of a problem that, although it had an initial economic impact, sought a solution to enable the people to freely trade monetary values. So much so that, at first, Bitcoin did not catch the attention of banks and, consequently, of governments.

To that end, the very recent historical picture - since Bitcoin has emerged in 2008 and, at least in legal science such a period is considered very small and almost historically irrelevant - demonstrates that the Blockchain protocol is revolutionary and can have application in almost everything that is related to electronic information.

To justify the relevance of this theme (data confidentiality) in the current scenario, is unnecessary. The development and entry into force of the General Data Protection Regulation demonstrates the importance and necessity of presenting solutions for Internet security issues, which will be addressed as a possible implementation of the Blockchain protocol for

protection and reliability of public data stored by governments.

Essential to improving security, there is also a greater data publicity for the circumscribed ones, since, as it will be understood, the Blockchain is a public book of electronic records, whose circulation of information can be tracked by all, regardless of the content. Hence, there are two spheres of action, one public and one private, as will it be developed later.

From the improvement presumed by the usage of the technology in question, there is, legally, the achievement of one of the goals of public service provision, which is efficiency. It is also a path for which there is not much alternative to the State, considering its technological development. Even though it is not given in the same proportion of the private world, it denotes absorption and adequacy also by the public sphere, although late and, within what we approached, the Blockchain protocol may soon become standard when it comes to information storage.

Thus, the thematic clipping of the present research is made. It will be pointed out the benefits that are presented with the use of Blockchain technology in the provision of the public service, especially regarding to the keeping of information of the most diverse public registries. Ergo, concepts and perspectives from authors from different areas will be explored, elucidating, as necessary, technical issues to enable the visualization of the achievement of efficiency of the public service in its most relevant developments.

2. The Utilities of the Blockchain Protocol beyond Bitcoin

Subsequently to the analyzes made in the first moment regarding the emergence and popularization of Bitcoin, with its peculiarities, objective and impact that it has been causing, it is time to move forward and think about the other possibilities that the technology can provide us, as many have already predicted and as some already do.

In the recent history, we have seen the problem with credit cards payment, for example, when a third person is needed to complete the transaction of money in web shops with bankers' costs, of course. This way, many technologies for digital money operations have been born and died unsuccessfully, as some researchers from Princeton University nominated over nineteen systems who recently proposed a digital economy (Narayanan, A. Bonneau, J. Felten, E. Miller, A. Goldfeder, S., 2016).

In Ametrano's words, Bitcoin naturally acquired the quality of digital gold, given the success it achieved. Consequently, what will be negotiated will be the other electronic currencies, whose foundation will be Bitcoin (Ametrano, F. M., 2016).

Bitcoin's inherent success is largely due to the tool used to ensure the rigidity and veracity of the money transfer information, which is known as the Blockchain protocol. Regarding this security, it is necessary to highlight the difference between the Bitcoin system and the exchange agencies, which are responsible for frequent reports of fraud and subtraction of electronic currencies. As mentioned in a different occasion (Teixeira, R. V. G., Da Silva, F. R., 2018), there is a gap between Bitcoin's encrypted system and the computerized information storage, and information system of exchange agencies, which use common, unprotected

servers and software. Unfortunately, in Brazil, the cases of fraud and theft of electronic currencies are frequent, but all related to the agencies and not to the Bitcoin system.

In any case, the Blockchain protocol not only guarantees veracity and uniqueness of monetary transactions. It also enables the development of systems that remodel the storage and flow of information on the Internet.

Moreover, Melanie Swan enlightened that the Blockchain is an application capable of functioning within the logic of Internet's protocol, providing immediate currency transaction and electronic payments. Besides, it will be proven useful not only for financial transactions, but also for any record service, recording, and monitoring. Therefore, the Blockchain is nothing but a great public book, which keeps a record of everything. It is capable of storing all the exchanges' information, be those of information or money, carried out among people all over the world to the end of it being used for registration, inventory, and exchanges, including any area of finance, economics, foreign exchange and property, as well as non-monetary issues such as voting, ideologies, reputation, political intentions, life, data, among others (Swan, M., 2015).

To visualize the suggested scenario, it is important to analyze, although limiting to the mere clarification, the operation of the Blockchain protocol. As it has been said, the Blockchain protocol is a part within the Bitcoin system by which the registration of information occurs immutably and without duplicity, consequently, reliably.

Bitcoin is a peer-to-peer currency that is not dependable of a central authority (Ulrich, F., 2014). The Blockchain is the technology by which all transactions are permanently registered, and unable to be reformed once the operation is carried out because the system information is all encrypted and stored in blocks' form. Thus, Blockchain means the grouped record of information movement, generally, with encryption.

Peer-to-peer means from point to point. The term expresses very well the idea considering that the connection occurs directly between the electronic devices of the users, without the intervention of a third manager, as in the previous systems in which there is the figure of an information administrator, a server.

Indeed, it is this decentralization that gives the system trustworthiness regarding its security against external attacks, since it would require the invasion of all connected devices to subtract or change the data inserted in it. The tool works by distributing the system information storage among the users themselves, without intervention or figure of a centralizing agent and controller of this information transit.

As for the Bitcoin', Alexandre Pacheco da Silva, using the lessons of Champagne, proposes an illustration that gives a more direct glimpse of how the operation is performed electronically, describing that:

"As a technology, Bitcoin has three elements that support its operation: (i) a public system of registration of its operations, called Blockchain, serving as an accounting book of entries and exits; (ii) an encryption algorithm called asymmetric encryption - associated with a

cryptographic proof-of-work - which is used to validate coin operations; and (iii) a computer network distributed in a decentralized way, according to the design of the users, also called miners, that verify and validate operations with the currency and update the public system of registers - Blockchain." (Da Silva, A. P., 2016).

In this perspective, it is evident the non-monocratic function of the Blockchain protocol, which is the technology that enables use beyond Bitcoin. Its operation and mainly its reliability call for the development and application of this technology in a diversity of systems. Especially those of digital processing and storage of data, which can serve to provide the public service, as previously defended.

In the present study, this is limited because of the unique scientific reasoning it proposes, noting that in many areas in the private sector the functionalities of the Blockchain protocol have been applied to stimulate the production of goods and services, as well as compliance issues, thus, in any automated process of market production.

Ergo, in the meantime, the Blockchain protocol should be considered for the development and improvement of the provision of services by the Public Administration, given the multiplicity of its utilities and applications, as it will be further explored.

3. The (un) Safe Internet

The security of the world-wide computer network is to be developed in a more favorable environment such as in theses and dissertations, that is, it is worthy of a much deeper study. Unfortunately, it will not be possible to fully exploit the question during the present research, due to the objective to be achieved, which is specifically related to public activity.

Now, the emphasis will be to elucidate the relevance that Internet security, or the lack of it, has acquired in recent years as a result of cyberattacks worldwide, focusing only on the social impact they have caused, even though they deserve economic and legal analysis as well.

The case of Wikileaks (Wikileaks, 2015) is emblematic because operations, strategic plans and information of the highest confidentiality of the American army were leaked and made available on a large scale by the world computer network. This fact was covered by the news from around the world, given the gravity and content of the acts then published and which has led to the arrest warrant of its founder, Mr. Julian Assange.

A great debate arose as to the secrecy of this type of institutional data as a counterpoint to people's right to information, that is, to know what is happening and what actions are taken by the public institutions. Finally, the founder of Wikileaks was accused of sexual abuse and arrested, being officially condemned by most national states. However, the organization continued to operate and other cases involving government secrecy were disclosed, including a large monetary contribution to the institution.

The report of this fact is important because, in spite of the fact that the event is worthy of its own research due to the innumerable implications that come from it, for us, it refers to a historical landmark in which the most forceful attention was given to the issue of security in the internet, especially concerning to governmental secrets, given the worldwide and

irreversible trend of digitalization of all state activity. Nevertheless, this sphere is not limited, since data and information are the true gold of the current digital society and having this type of occurrence also implicated in private orbit.

Other cases deserve attention, such as that of the US presidential candidate, Hilary Clinton (New York Times, 2016), who had campaign emails posted on the Wikileaks platform. In the same vein, the leak of contacts and information exchange between the American candidate Donald Trump's son and the Russian secret service, also contributed for the controversial and polemic American elections (New York Times, 2017).

Furthermore, and perhaps more prominently, the ransomware carried out against several entities in an attack of global proportions, whereby a virus called WannaCry invaded and froze access to data of public and private companies, demanding the payment of redemptions in crypto-coins (Folha de S ão Paulo, 2017).

Other attacks against specific institutions are also worth mentioning. The one against the Walt Disney Picture, in which intruders threatened to release a film not yet released from the studio (Telegraph, 2017), and the one against Netflix, threatening, in the same sense, to offer audiovisual product not yet released by the streaming tool (Telegraph, 2017).

Although there are many other examples of cybercrime that have put Internet safety on the line, the last to be mentioned in this research will be the one of the Ashley Madison platform. This platform contributed for users to meet with people who sought extramarital affairs. The platform was targeted by hackers, with the exposure of users' names and some personal data and free access by anyone on the internet (The Guardian, 2015).

Not to mention the recent episode involving the sale of personal information and data of Facebook's users to Cambridge Analytica, which would have helped in Trump's presidential campaign.

In summary, what it is proposed to demonstrate is the fact that Internet security demands heated debate due to its destructive capacity, since practically every citizen of the planet can be affected, directly or indirectly.

The examples are mentioned in a gradation, seeking to raise awareness that not only governments and large corporations are in danger. The last-mentioned cases are very important, and they stand out because they report damages to common and anonymous users, who do not have, in the clear majority, technical conditions to even know how to scale the risks assumed when using an application or any device on the internet. Contextualizing to the proposed theme, the security and protection of personal data on the Internet is also a state obligation.

This is what Professor Ronaldo Lemos concludes by mentioning that: "As our lives become increasingly digital, themes such as privacy, freedom of expression, innovation, entrepreneurship, the very idea of development, will increasingly appear through the Internet. For this reason, the protection of principles such as net neutrality, as well as the translation of the principles of the Federal Constitution into the reality of the network, is becoming more

and more essential" (Lemos, R., 2014).

The storage of information in electronic devices or even in the cloud, has been the great target of digital criminals. Public databases, in this sense, are also subjected to being victims of this type of illegal action.

The circumstance is aggravated even more when we are faced for example, in Brazil, which follows the world trend, with the attempt to create a single citizen's record.

The risk is unimaginable. We cannot measure how the "disappearance" of data stored in a particular public office would be or worse, the damage that can be caused to circumscribers who have all their data leaked onto the world computer network, such as card cloning, bank account invasion, transfer of property (which will soon be possible to be done by increasingly popular digital signatures), acquisition of unintended goods and services, among other crimes that may be committed with possession of personal data, highlighting the increasing tendency of dispensation of the physical presence to perform legal acts of civil life.

Thus, the demand of digital data storage mechanisms in need of greater protection is emphasized, even more when regarding information from public agencies.

Therefore, we will try to highlight the use of the Blockchain protocol as a possible tool to provide greater security to the Public Administration and to the personal data of the jurisdictional ones. It is up to the State to seek the service provision in an efficient way, considering efficiency as a "way of organizing, structuring, disciplining Public Administration [...] with the same objective of achieving the best results in the provision of the public service" (Di Pietro, M. S. Z., 2007), while the public service will only do so if capable to ensure user safety.

4. The Use of the Blockchain Protocol to Guarantee Efficiency in the Provision of Public Services

Having described the current scenario, whose storage and information flow is predominantly through the Internet, as opposed to the vulnerability of the network, it is necessary to develop applications that in some way combat possible attacks and thus, bring security to users of the network. The users may be all individuals on the planet, since we are directly or indirectly affected by cyberattacks as is seen in the examples previously mentioned. Even more so when we are also faced with the irreversible tendency of digitization of the Public Power's activities, especially regarding data processing.

In contrast to this fragility, Bitcoin emerges along with one of its operating components, the Blockchain protocol, which provides rigidity and inviolability to the system that promotes transfer of values that are nothing more than electronic information.

Hence, this technology can be used by the Public Administration in the storage of public data, as well as in the management and, especially, security of the data related to the circumscribed in the most diverse areas such as civil registry, registry of legal person and natural person, passport, voter registration card, driver's license, income tax, real estate property and other movable property. To sum up, all public life of the citizen.

It should be noted that the creation of a single identity card (Brasil, 2017) has already been legislated in Brazil, for which several previously separate documents have already been grouped (RG-Identity Register, CPF-Physical Persons Registry, CNH-driver's license and Voter's registration Card). It is also worth mentioning that this measure is not exclusive to this country since single documentation has already been a reality in other countries for quite some time.

Yet, what is important to highlight is that there will already be a single data record of the citizen, although other data types such as property and income statements could be included. Such data will be stored in traditional servers, which are more vulnerable to possible hacking, according to examples already quoted. Besides, the traditional servers demand much higher maintenance costs than the Blockchain protocol can offer.

According to the analysis of the public administration's goals – wherein Brazil was considered an example, but in which is possible to see a worldwide trend of online data storage -, in contrast to the storage and security capacity of the Blockchain protocol, it is pointed out that implementation of the latter is indeed feasible.

The idea of digitalization may be frightening in more traditionalist and cautious cultures regarding the reliability of electronic systems. In Brazil, however, where the electoral process is all digitalized, there is not so much resistance to implementing a fully digital system.

Don Dapscott and Alex Dapscott write about the possibility of governments use the technology in question, and the more restrictive position adopted by some, while others see the possibility of advancement in its use:

"Regulators have also snapped attention, establishing task forces to explore what kind of legislation, if any, makes sense. Authoritarian governments like Russia's have banned or severely limited the use of Bitcoin, as have democratic states that should know better, like Argentina, given its history of currency crises. More thoughtful governments in the West are investing considerably in understanding how the new technology could transform not only central banking and the nature of money, but also government operations and the nature of democracy. Carolyn Wilkins, the senior deputy governor of the Bank of Canada, believes it's time for central banks everywhere to seriously study the implications of moving entire national currency systems to digital money. The Bank of England's top economist, Andrew Haldane, has proposed a national digital currency for the United Kingdom." (Tapscott, D. Tapscott, A., 2016).

There are already suggestions for adapting Blockchain technology to create systems that protect personal data, as we can see in the work of Guy Zyskind, Oz Nathan and Alex 'Sandy' Pentland, who have technically developed a way to guarantee personal data security through distribution of the information store (Zyskind, G. Nathan, O. Pentland, A., 2015).

It is evident that the public sector has specific characteristics that require adaptation in the implementation of actions such as the one suggested in this opportunity. Among them, for example, are the limitations regarding the direct contracting of suppliers of goods and services. Though, given the magnitude of the chance of resolution or at least the great

improvement in the security of public data, such issues should be subrogated to the highest order of general benefit, and no limitation of an ordinary nature should prevail.

A certain objection that may exist between the government to adopt the technology in question must be mentioned, since a greater publicity of the administrative acts is inherent to the use of the Blockchain. As some have suggested, politicians may be the biggest impairment to the implementation of the Blockchain by the Public Administration, as it may mean easier scrutiny of state activity (Economist, 2017).

Such resistance may come from future predictions, such as the one made by Melanie Swan, who believes storing civil information in Blockchain can, over time and through global deployment, can relativize the very essence of the State. That way, through the unification of records, there would only be citizens of the world, being the country of origin only a place of origin, and not determining and characterizing the individual as it is today.

The record would be based on the unification of databases spread throughout the world in which all information of every person would be available to all, as well as transfer of goods and coins would be given unrestricted (Swan, M., 2015).

The idea is of a futuristic society, to which one can go or not. In a short period, however, the implementation of the Blockchain protocol for the storage and processing of public data, although individually among States, may mean protection and security of data.

The benefits enable a change from the greater system's inviolability to the veracity and non-duplicity of the information registered through the Blockchain protocol, allowing, immediately, greater security and consequently more efficiency of the public service.

5. Conclusion

The Blockchain protocol is the most important instrument with the emergence and popularization of Bitcoin. It is through this that it was possible to give security to the veracity of the information fed to the system. With its help, the duplication or reapplication of the same transaction was prevented.

As we have seen, the system operates through applications with high encryption, as well as distribution of information storage. In other words, there is no central server in which the data and operations are stored, having the information stored immediately between the users themselves, and giving the connection through peer-to-peer logic.

Notwithstanding the technical issues that best explain this operation, of which it has been warned not to attempt analysis and exhaustion, the implications and possibilities that the development of this technology possess have an effect, and soon it will be the great tool of a new technology revolution, like the internet has been since the 1990s.

Given the security of information and protection against external attacks, it is striking that such an instrument can also serve the Public Administration. The storage and flow of data and information of public banks could take advantage of the Blockchain protocol after some adjustments. In addition, it could unify civil documents, to enhance consultation of citizens'

information, which has implications for others public agents as well as individuals, such as for consultation of assets and debts of someone before conducting a business or for criminal background check by jurisdictions of another region.

It is obvious that the possibilities and legal implications, as well as technical ones, are worthy of a deeper study, which unfortunately cannot be done in this opportunity.

The fact is that the Blockchain protocol has already been studied and implemented by numerous private institutions, given the cost benefits (mainly with electric power to support traditional servers), and especially given the security provided due to the inviolability and veracity of information contained in data storage and processing systems.

On the legal side, the possibility of using blockchain protocol technology for public administration is justified because public service efficiency is an objective to be achieved by the State. Therefore, it has been shown that the protocol can provide greater security and reliability of data and information of public scope, which unquestionably means making such a service more efficient.

Ergo, the hypothesis must be discussed, albeit in internal chamber, in order to achieve a safer and more efficient public service, in view of the potential offensive of insecurity on the Internet that we witness nowadays.

Acknowledgement

References

Ametrano, F. M. (2016). *Hayek Money: The Cryptocurrency Price Stability Solution*. SSRN. https://dx.doi.org/10.2139/ssrn.2425270

Brasil. (2017). Federal Law n. 13.444/2017. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13444.htm>. Accessed in Jun. 17, 2018.

Da Silva, A. P. (2016). *Oportunidades e oportunismos: dimensões interna e externa da segurança do Bitcoin. In:* A revolução das Moedas Digitais: Bitcoins e Altcoins. Barbosa, T. C. B. M. (org.). São Paulo: Editora Revoar. p. 42.

Di Pietro, M. S. Z. (2007). *Direito Administrativo*. 20th ed. São Paulo: Atlas. p. 74.

Folha de São Paulo (2017). Available at: <http://www1.folha.uol.com.br/mundo/2017/05/1883408-mega-ciberataque-derruba-sistemas -de-comunicacao-ao-redor-do-mundo.shtml>. Accessed in Jun. 15, 2018.

Lemos, R. (2014) *O Marco Civil como símbolo do desejo por inovação no Brasil. In:* Marco Civil da Internet. Leite, G. S., Lemos, R. (org.). São Paulo: Atlas. p. 11.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and*

Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press. p. 10-11.

New York Times. (2016). Available at: <https://www.nytimes.com/2016/10/10/us/politics/hillary-clinton-emails-wikileaks.html>. Accessed in Jun. 14, 2018.

New York Times. (2017). Available at: <https://www.nytimes.com/2017/11/13/us/politics/donald-trump-jr-wikileaks-emails-democrats.html>. Accessed in Jun. 15, 2018.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Inc. p. 10-11.

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin. p. 86.

Teixeira, R. V. G., & Da Silva, F. (2018). *Bitcoin e a (Im)possibilidade de sua proibição: Uma violação à soberania do Estado?*. *Revista Brasileira de Políticas Públicas, 7*, 106-121. https://dx.doi.org/10.5102/rbpp.v7i3.4935

Telegraph. (2017). Available at: <https://www.telegraph.co.uk/films/2017/05/16/hackers-demand-ransom-disney-pirates-caribbean-5/>. Accessed in Jun. 15, 2018.

Telegraph. (2017). Available at: <https://www.telegraph.co.uk/news/2017/05/01/broadcasters-fear-release-hit-shows-dark-overlord-claims-leak/>. Accessed in Jun. 15, 2018.

The Guardian. (2015). Available at: <https://www.theguardian.com/technology/2015/aug/19/ashley-madison-hack-outcome>. Accessed in Jun. 16, 2018.

Ulrich, F. (2014). *Bitcoin: a moeda na era digital*. São Paulo: Instituto Ludwig von Mises. Brasil. p. 17.

Wikileaks. (2013). Avaliable at: <https://wikileaks.org/What-is-Wikileaks.html>. Accessed in Jun. 14, 2018.

Zyskind, G., Nathan, O., & Pentland, A. (2015). *Decentralizing Privacy: Using Blockchain to Protect Personal Data*. IEEE. https://dx.doi.org/10.1109/SPW.2015.27

Copyright Disclaimer